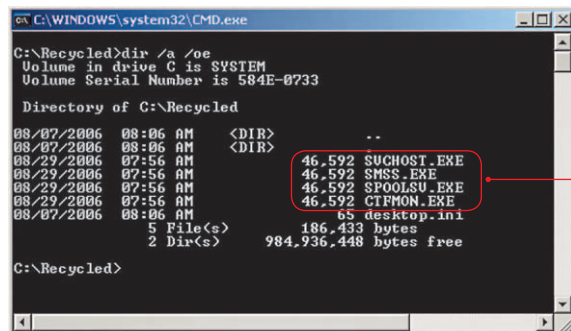
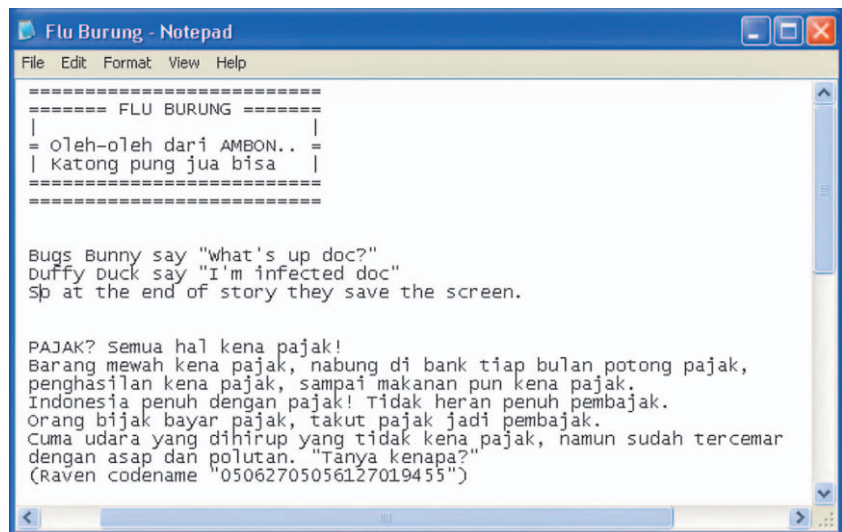
Waspada H5N1 Menyerang Komputer

Jangan biarkan komputer Anda terserang flu, seperti yang dialami oleh komputer milik salah satu pembaca *PC Media* ini. Apalagi bila flu tersebut bukanlah penyakit flu biasa, tapi flu burung atau H5N1. Ternyata penyakit yang mematikan bagi unggas dan manusia ini dapat menular juga pada komputer Anda.

Arief Prabowo

Pesan dari pembuat virus.

Mungkin Anda sedikit bingung dengan pernyataan di atas. "*Lho*, bagaimana bisa komputer terkena virus flu burung?" Jawabnya, ya bisa saja. Tapi virus yang ini bukanlah virus flu burung biologis seperti yang menyerang pada unggas dan manusia.

Hanya satu persamaan yang ada antara virus flu burung biologis dengan yang ini, yakni sama–sama menular. Virus flu burung yang akan dibahas kali ini adalah sebuah virus komputer yang dapat menulari atau menginfeksi dokumen–dokumen Microsoft Word Anda dengan caranya sendiri yang boleh dibilang beda dengan virus–virus lokal yang sekarang semakin heboh. Penasaran seperti apa? Ikuti terus bahasannya kali ini.

File induk virus yang bersembunyi di direktori "Recycle Bin".

Apa Ciri-ciri dari FluBurung?

Virus yang memiliki icon mirip seperti Microsoft Word ini memiliki ukuran tubuh sebesar 46.592 bytes. Di-*compress* menggunakan tool executable compressor ASPack dan menggunakan sedikit teknik enkripsi. Seperti kebanyakan virus lokal lainnya, virus ini diprogram menggunakan bahasa favorit para *virus maker*, yakni Visual Basic. Pada *resource* yang ada di tubuh virus ini, terdapat icon–icon Ms. Word dan *version information* yang dibuat sedemikian rupa agar mirip dengan aplikasi Ms. Word yang tentunya agar user tidak curiga. Selain itu, terdapat juga *resource* dengan nama FLU_BURUNG, yang setelah di-*unpack* resource ini berupa *text* biasa yang merupakan pesan dari pembuat virus. Dan apabila virus ini menginfeksi dokumen Ms. Word Anda, extension-nya menjadi .scr, yang secara *default* merupakan extension untuk file Screen Saver.

Bagimana Ia Menginfeksi?

Pada saat kali pertama aktif, yang dilakukannya adalah memeriksa apakah sistem tersebut sudah pernah diinfeksi? Apabila belum, maka ia akan menginfeksinya. Cara yang dilakukannya cukup unik, yakni memeriksa apakah pada direktori *Recycle Bin* sudah terdapat "agen" dari sang virus. Kalau belum, dengan senang hati ia akan segera meng-*copy*-kan tubuh asli dari sang virus ke direktori Recycle Bin tersebut yang secara default direktori tersebut sebenarnya bernama Recycled dan biasanya akan terdapat pada setiap drive harddisk.

Hal yang telah dilakukannya ini memang berbeda bila dibandingkan virus lokal lainnya, karena ia memilih folder Recycle Bin sebagai "rumah"-nya dan bukan di direktori windows atau system. Cerdik memang, apalagi file yang sengaja di-copy ke direktori Recycled ini, tidak dapat terlihat begitu saja. Nama file induk yang digunakan pun mirip sekali dengan nama–nama process atau service penting dari Windows yakni CTFMON.EXE, SMSS.EXE, SPOOLSV.EXE, dan SVCHOST. EXE. Apabila tubuh virus dilihat menggu-

nakan hex editor, data mengenai nama–nama file induk-nya tidak dapat dibaca dengan mudah begitu saja, karena seperti yang dibilang di awal, virus ini menggunakan sedikit teknik enkripsi.

Hal ini juga berlaku bagi beberapa *string* lain, seperti *key, section*, ataupun item di registry yang ia ubah. Dan setelah file induk berhasil ditanamkan pada sistem tersebut, ia akan mengubah registry agar dapat otomatis aktif pada saat memulai Windows, yang salah satunya terletak pada HKEY_CURRENT_USER, SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell. Pada sistem yang telah terinfeksi juga akan terdapat pesan dari pembuat virus pada direktori Temporary.

Selain itu, tubuh virus ini juga memiliki nilai *hashing* yang berbeda-beda, karena setiap ia membuat duplikat dari dirinya, ia akan membuat nomor acak yang akan diletakkan pada akhir tubuh aslinya sebanyak 4 bytes.

Teknik Enkripsi

Dengan bermodalkan salah satu string yang terdapat di tubuh virus tersebut "MS\fI\Y\UN", akhirnya ketemulah enkripsi yang digunakan. Sangat sederhana, yakni hanya memundurkan setiap nilai karakter ASCII sebanyak 7 karakter. Dan dengan membuat program kecil yang akan mendekripsikan seluruh string yang terenkripsi, maka didapatkan hasil bahwa string "MS\fI\Y\UN" adalah "FLU_BURUNG".

Infeksi File DOC

Sebenarnya banyak hal menarik yang dilakukan oleh virus ini. Salah satunya lagi adalah dengan menginfeksi setiap *document* Ms. Word yang baru saja dibuka. Seperti yang kita ketahui bahwa apabila kita membuka suatu dokumen, entah itu file txt, rtf, doc, ataupun yang lainnya maka windows menyimpan *history* atau *recent document* mengenai file apa saja yang pernah dibuka. Anda dapat dengan mudah melihatnya dengan mengklik "Start>Documents". Dan itulah yang dilakukan oleh virus ini. Ia akan mencoba mendapatkan direktori asli yang menyimpan informasi recent document, yang secara default terletak pada direktori "\Documents and Settings\%UserName%\Recent" lalu membaca isi dari direktori tersebut. Apabila terdapat link yang mengarah ke file .doc maka dengan sigap virus ini akan menginfeksikannya.

Teknik infeksi yang digunakan adalah dengan cara menambahkan file dokumen asli ke bagian akhir dari tubuh asli virus. Dan menggunakan nama yang hampir mirip dengan aslinya, yang membedakan hanya ektensionnya, yakni .scr. Sementara dokumen yang asli disembunyikannya dengan memberikan *attribut hidden*.

Jelas saja apabila file yang sudah terinfeksi virus tersebut Anda coba buka paksa dengan Ms. Word, maka tidak akan bisa karena formatnya berbeda, bukan lagi file Ms. Word tapi menjadi Executable. Tapi kalau Anda klik ganda file yang terinfeksi tersebut, dokumen tersebut dapat terbuka dengan baik pada Ms. Word. Sebenarnya cara kerjanya cukup sederhana, yakni pada saat menjalankan dokumen yang terinfeksi, virusnya terlebih dahulu yang akan memegang kendali, lalu ia akan mencoba mengeluarkan data yang merupakan dokumen Ms. Word tadi yang ada di akhir tubuhnya dan diletakkan pada direktori ia berada. Lalu menjalankan dokumen yang berhasil dikeluarkan dari dalam tubuhnya itu.

Mengubah registry

Karena extension file yang digunakan pada saat menginfeksi file adalah .scr, jadi virus melakukan banyak perubahan untuk extension ini di registry, tujuannya jelas untuk menyamarkan kehadirannya. Seperti pada *type information* dari "Screen Saver" menjadi "Microsoft Word Document". Dan masih banyak beberapa key atau item lainnya yang ia ubah.

Tidak seperti virus lainnya yang selalu men-*disable* beberapa opsi penting pada Windows seperti MsConfig, Regedit, Command Prompt, Folder Options, dan lain sebagainya, pada virus ini hal tersebut tidak dilakukan. Namun untuk Folder Options, yang ia lakukan adalah mengeset default UncheckedValue untuk HideFileExt dan SupperHidden, jadi walaupun kita mencoba masuk ke Folder Options untuk mengubah settingan-nya, tidak akan berpengaruh apa–apa. Karena tetap saja Windows tidak menampilkan extension dan file dengan attribut hidden.

Dan pada key "HKEY_CLASSES_ROOT*" virus juga melakukan beberapa perubahan pada item QuickTip, TileInfo, dan InfoTip.

Stay Resident in Memory

Pada saat virus aktif, maka ia akan bersemayam di memory dan memonitor aksi yang dilakukan oleh user. Di memory, virus ini memiliki tiga process atau lebih, dengan nama yang sama seperti file induknya. Apabila ada yang mencoba untuk membunuh process-nya, dengan segera ia akan memanggil kembali process yang telah di-*kill* tersebut. Hal tersebut juga berlaku untuk item *autostart* virus di registry. Otomatis akan dibuat ulang apabila ada yang mencoba menghapusnya dari registry.

Selain itu, tugas virus yang lebih penting lainnya adalah memonitor folder "Recent Documents", karena ia akan segera menginfeksi setiap ada dokumen yang baru dibuka.

Membasmi FluBurung

Yang agak *ribet* dalam membasmi virus ini adalah mendisinfektan file dokumen Ms Word yang telah tertular oleh virus FluBurung ini. Maka dari itu, bila komputer Anda terinfeksi, silakan menggunakan PCMAV RC8 untuk membersihkannya, namun tidak ada salahnya untuk membuat backup-nya terlebih dahulu, untuk menghindari hal-hal yang tidak diinginkan. Namun apabila PCMAV tidak dapat mengenali virus FluBurung tersebut, silakan Anda kirimkan sampel virusnya kepada kami. Kami tunggu! ■

Beberapa file dokumen Ms. Word asli dan yang telah terinfeksi.